Back to Contents

GIF-011-00

Generation IV Roadmap

Crosscutting Risk and Safety R&D Scope Report

Issued by the Nuclear Energy Research Advisory Committee and the Generation IV International Forum

December 2002

MEMBERS OF THE RISK AND SAFETY CROSSCUT GROUP

Per Peterson	Co-chair	University of California–Berkeley, United States
Marc Delpech	Co-chair	Commissariat à l'Energie Atomique, France
Paul Pickard	Technical Director	Sandia National Laboratory, United States
Sydney Ball		Oak Ridge National Laboratory, United States
Bernard Ballot		Framatome – ANP, France
Jeff Binder		Argonne National Laboratory, United States
Dennis Bley		Buttonwood Consulting
Charles Boardman		Consultant
Mario Carelli		Westinghouse, United States
Marco Gasparini		International Atomic Energy Agency, United Nations
Kazuyoshi Kataoka		Toshiba Corporation, Japan
Stephen Rosen		Consultant
Jacques Royen		Organisation for Economic Cooperation and Development—Nuclear Energy Agency, Europe
Kune Y. Suh		Seoul National University, Korea

OTHER CONTRIBUTORS

Douglas Chapin	GRNS Representative	MPR Associates, United States
Madeline Feltus	DOE Representative	Department of Energy, United States
Gian-Luigi Fiorini	RIT Representative	Commissariat à l'Energie Atomique, France

CONTENTS

FIGURES

TABLES

CROSSCUTTING RISK AND SAFETY R&D SCOPE REPORT

1. INTRODUCTION

The Risk and Safety Crosscutting Group (RSCG) has developed recommendations for research areas that are relevant to the viability and performance assessments of future nuclear energy systems in meeting the Generation IV Safety and Reliability (SR) goals.

Under SR Goal 1, SR research focuses on those events of relatively high to moderate frequency that affect worker safety, facility reliability and availability, and the frequency of accident initiating events. Under SR Goal 2, SR research focuses on those low probability event sequences that can lead to core degradation, or in other facilities, to the release of radionuclides from their most immediate confinement, or to nuclear criticality with risk for undue exposures. Under SR Goal 3, SR research focuses on those very low probability accident sequences where significant core degradation or other release could occur, and the performance of additional mitigation measures that reduce and control releases outside the facility and doses to the public.

The RSCG review of the detailed viability Research and Development (R&D)needs for the individual Generation IV concepts, given in the technical working group (TWG) R&D Scope Reports, shows that there exist few SR viability research issues that crosscut multiple concepts, primarily because viability issues tend to involve unique and less understood characteristics of specific concepts. Those crosscutting issues that do emerge arise primarily in SR Goal 3, and in the requirement to have a consistent methodology for SR viability assessment of concepts where detailed design information is not fully available.

Different nuclear energy systems employ different strategies to meet the specific SR goals. Some strategies can be relatively simple, and such simplicity can create narrower uncertainty bounds for safety performance, even for relatively immature system designs. More complex strategies may have equal or greater potential, but depending upon the level of testing, development, and relevant operating experience currently available, likely also have wider uncertainty bounds. The Final Screening process gave substantial credit to those reactor systems that adopt simple and robust approaches for achieving the primary safety functions of reactivity control, decay heat removal, and radionuclide confinement. The Final Screening therefore identified concepts that provide a strong foundation—particularly from the perspective of human factors—for building future Generation IV nuclear energy systems.

In the last three decades there have been major advances in the ability to predict and control the reliability and safety performance of nuclear systems. These improvements have come from technology innovations ranging from improved sensors to more robust component designs; from improved experimental methods and a growing body of experimental data; from improved modeling tools and methodologies for quantifying uncertainty; and from improvements in licensing, construction, operations, and maintenance methods as well as lessons learned from experience. Modeling advances have also made it possible to better quantify the uncertainty in the prediction of the response of facilities to transients and accidents, allowing a shift away from bounding and unproductively conservative analysis, toward best-estimate analysis with quantitative assessment of uncertainty. Improved understanding of human factors, and the consideration of human factors at every stage of design and operation, starting with the selection of process technologies that avoid complex physical interactions to the final optimization of the man-machine interface, will further increase the potential of Generation IV technologies.

By the end of Viability phase R&D, each system must have a safety case that identifies initiators and strategies for response. A standard methodology is needed to provide a consistent evaluation with respect to the Generation IV safety goals for these different strategies.

Within the framework of this methodology, the capability to accurately calculate safety margins, and the uncertainty in these margins from all sources, will play an important role in the Viability and Performance evaluations of Generation IV concepts, because it will provide a quantitative basis for optimizing concept design features.

1.1 Definitions for SR Viability and Performance Research

SR viability research involves crosscutting topics that will play an important role in the viability evaluation of Generation IV concepts. These viability research topics focus in two areas. The first is generated by goal SR3, which seeks changes in offsite emergency planning methods that go significantly beyond the experience available in the licensing of Generation II and III reactors. The second provides tools— transient analysis methods and simplified probabilistic risk assessment—that can be used for the SR viability evaluations of Generation IV concepts.

SR crosscutting performance research can enhance the capability of Generation IV systems to better meet the SR goals. Seven broad areas of research exist where such improvements are possible. Importantly, most of these improvements would also benefit the designs of near-term deployment reactors.

1.2 SR Viability Crosscutting Research

At the time that SR viability evaluation occurs for a given Generation IV concept, the design of the reactor and fuel cycle facilities must have sufficient detail to allow comprehensive description of the implementation of the lines of defense which provide defense-in-depth, including measures available to mitigate the consequences of core and plant degradation during design extension conditions (formerly Beyond Design Basis); to allow the use of simplified probabilistic risk assessment (PRA) to identify design-basis accidents and transients as well as the highly hypothetical sequences; to identify and rank

Level of design detail required for SR Viability Evaluations

For SR Viability Evaluation, the level of design detail for reactor and fuel cycle facilities should be sufficient to allow:

- Description of the facility design features that implement the five individual levels of defense as defined by INSAG-10 (see Table 1)
- Performance of a simplified PRA to accurately quantify the contribution to the risk of all the design-basis transients and accidents resulting from internal and external events, for all facilities and all operating modes and assess their approximate probabilities
- Identification and ranking of the phenomena that govern the system transient response under design basis and design extension conditions
- Demonstration that separate effects experimental data are available, or are planned for, that closely replicates the scaled boundary and initial conditions for the dominant phenomena with minimal distortion
- Performance of selected best-estimate design-basis transient and accident analyses demonstrating the quantitative evaluation of uncertainty, and explicitly identifying approximations and assumptions that will be removed by subsequent performance R&D
- Description of the integral test facilities and their instrumentation planned to validate system transient response models, preferably at prototypical scale.

phenomena of importance to transient response and to specify experimental information required to validate transient models. The table summarizes the level of design detail required for this evaluation.

The four specific areas recommended for SR viability R&D are:

- S*ystem optimization and safety assessment methodology*. Generation IV viability evaluations will be performed with incomplete design information. For these evaluations, the deterministic concept of defense-in-depth needs to be integrated with simplified probabilistic considerations such as systems reliability, probabilistic targets, etc., to provide metrics for acceptability and a basis for additional requirements, and to ensure a well balanced design. This methodology must explicitly identify the assumptions and approximations used in the simplified process, to assure that these assumptions and approximations are addressed during performance R&D. Several Generation IV concepts have unique, new assessment issues. For example, many employ passive safety characteristics and systems to a much greater extent than current nuclear facilities. The failure of passive components requires a complex combination of physical and human factor ingredients. Current probabilistic risk assessment methods are not well adapted to the assessment of passive safety systems where all components have very small predicted failure probabilities, and where operating data is sparse or would not be expected to provide statistically useful information,

- *Develop a simplified PRA methodology.* The methodology needs to integrate passive and active safety functions. The Code Scaling, Applicability, and Uncertainty method can in principle treat such problems, but has thus far been applied primarily to LWRs and requires more extensive design and modeling information than is available at the Viability Evaluation stage. Modeling Generation IV systems requires improved approaches to understand events that arise from incomplete knowledge of potential system interactions and human factors. Research focused on the factors which affect the reliability, and ability to predict reliability, of passive safety components and interactions between components has the potential to improve quality of the viability evaluations of the Generation IV concepts. In addition, such a methodology should take into account coupling of Generation IV nuclear systems to alternative energy product plant systems.

- *Emergency planning methods (EPM).* By virtue of their relatively small accident source terms, very slow transient response, low uncertainty in accident phenomenology, and extremely low probability for the scenarios resulting in significant offsite radionuclide release, several Generation IV concepts could potentially benefit from emergency planning tailored to their characteristics. Specifically, it has been proposed that Emergency Planning Zone (EPZ) radii or other planning actions different than those used for existing reactors, as well as alternative severe accident mitigation methods such as filtered confinements, could be appropriate for some of the Generation IV concepts.

- *Define the technical basis underlying existing emergency planning.* These results should then be used to establish methods for the design and analysis of Generation IV plants to demonstrate that all design basis transients, accidents, and design extension conditions have been identified, that transient analysis has sufficiently low uncertainty, and that defense-in-depth has been implemented robustly, so that protective action guidelines for modified emergency planning requirements can be met. The approach should be developed in coordination with national regulators and other responsible authorities, such that agreement in principal can be obtained.

1.3 SR Performance Crosscutting Research

The RSCG has identified additional SR technology R&D domains where advances have the potential to improve the SR goal performance of most or all Generation IV facilities. These domains

could provide fruitful areas for crosscutting Generation IV Performance R&D, and many of these domains will likely be studied under near-term deployment research for application to near-term systems. These are:

- *Licensing and Regulatory Framework.* Many Generation IV systems involve substantial changes in safety-system design and implementation that require licensing implementation significantly different from current experience. Best estimate and risk-informed bases for licensing will play a stronger role, due to the greater simplicity and improved uncertainty characterization for the new safety systems. Develop more flexible, risk informed regulatory tools for licensing of these advanced systems, and for increasing international consistency in design for licensing. Significant improvements are expected for the whole plant's optimization and economy (e.g. through an adequate classification methodology).

- *Radionuclide Transport and Dose Assessment.*. Develop improved phenomenological and real-time transport and dose modeling methods. This would support improved real-time emergency response, as well as optimized emergency planning methods and requirements.

- *Instrumentation, Control, and the Human-Machine Interface (IC&HMI).* Develop improved sensors, data acquisition and processing, intelligent information systems, and human interface design. All these IC&HMI topics will contribute to improved system reliability, availability, and safety.

- *Reactor Physics and Thermal Hydraulics.* Improve the quantitative assessment and minimization of uncertainty in transient system modeling by advancing phenomena scaling methods, improved physically based models for fundamental phenomena, advanced computational capabilities, improved numerical methods and approaches to discretization, and improved methods for uncertainty quantification.

- *Risk Management.* Improve decision making methods for activities such as system design, construction, routine operations and maintenance (O&M), off-normal operation, and accident management by improved PRA methodologies, component databases, and coupling of probabilistic and deterministic methodologies to incorporate more sophisticated phenomenological models and human factors considerations.

- *Operation and Maintenance.* Augment the reliability, availability, and safety of Generation IV facilities with improved component designs, predictive maintenance methods, advanced information technologies, and incorporation of human factors and safety culture considerations during the design.

- *Human Factors.* Develop methods to improve system optimization for human factors at every stage of system design, starting with fundamental process selection, to detailed implementation of instrument and control (I&C) and the human-machine interface (HMI).

1.4 SR Additional Recommendations

During the Final Screening process, the RSCG provided guidance on the consistency of scoring between concepts. Due to the limited information on the detailed design of most of these concepts, this review focused on intrinsic characteristics of the concepts that could affect their potential for performance in the SR goals, such as the thermal inertia associated with reactor cores. Such intrinsic characteristics provide a strong foundation, but still play only a partial role in the safety and reliability of nuclear energy

systems. The details of the facility designs and the fundamental safety architecture also have high importance to safety and reliability. The benefits of the current state-of-the-art in the seven SR technology R&D areas, as well as further advances during performance research, can only be realized if these advances are actually incorporated into the detailed design of Generation IV facilities. This leads to a general RSCG recommendation:

> "Generation IV research on specific concepts should include an effective Safety and Reliability peer-review mechanism. This review process should be structured to ensure that the best SR design practice is employed in all Generation IV facilities, with a particular focus on the correct implementation of defense-in-depth principals. These reviews can be integrated with the Viability and Performance Evaluations, but need to include experts in each of the seven primary SR performance technology areas. The reviews need to be structured so that the results of each review feed back into the detailed Generation IV concept design."

Table 1. Levels of defense-in-depth (INSAG-10).

Levels of Defense-in-depth	Objective	Essential Means	Generation IV Goals
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Safety and Reliability-1. Generation IV nuclear energy systems operations will excel in safety and reliability.
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures	Safety and Reliability-2. Generation IV nuclear energy systems will have a very low likelihood and degree of reactor core damage.
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management	Safety and Reliability-3. Generation IV nuclear energy systems will eliminate the need for offsite emergency response.
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Offsite emergency response	

The three Generation IV SR goals align with the broadly applied concept of the IAEA's definitions of levels of defense-in-depth, as summarized in Table 1 and in detail in the SR section of the EMG Final Screening Methodology Report, Appendix A.

The following chapters discuss issues specific to each of the SR goals, and the primary research areas that crosscut each of the R&S goals. A series of appendices summarize key areas for Generation IV performance research.

2. SAFETY AND RELIABILITY (GOAL 1)

Goal Statement:

Safety and Reliability-1 (SR1). Generation IV nuclear energy systems operations will excel in safety and reliability.

Goal SR1 focuses on safety and reliability during normal operation of all facilities in the nuclear energy system, from mining to the final disposal of waste. Thus the focus is on those high to medium probability events that set the forced outage rate, control routine worker safety, and result in routine emissions that could affect workers or the public.

Because SR1 focuses on high to medium probability events, analysis of SR1 performance can take advantage of statistical data for the reliability of equipment and for the frequency of human errors and other factors that affect system reliability. Probabilistic risk analysis provides an important tool for quantitatively predicting reliability, and of equal importance, for identifying design and operation features that can enhance reliability and reduce the frequency of accident initiating events.

All seven of the SR research areas play important roles in the performance of nuclear energy systems. The licensing and regulatory framework creates important boundary conditions on facility O&M, in particular through the Technical Specifications which define operating limits for facilities. Radionuclide transport and dose assessment is applied to understand, characterize, and minimize routine worker exposures and environmental releases. Instrumentation and control systems play key roles in plant reliability, and human factors affect all aspects of plant O&M. Reactor physics and thermal hydraulics control normal plant operation, as well as the evolution of normal transients such as start-up and shut-down. O&M activities directly affect safety and reliability through methods such as predictive maintenance.

3. SAFETY AND RELIABILITY (GOAL 2)

Goal Statement:

Safety and Reliability-2 (SR2). Generation IV nuclear energy systems will have a very low likelihood and degree of reactor core damage.

Goal SR2 identifies facility attributes that, using models and experiments, create high confidence that all design basis accidents (DBA) are correctly managed and that reactor core damage will have a very low likelihood or can be excluded or practically excluded by design (and in other facilities, that the release of radioactive material from its most immediate confinement or nuclear criticality cannot occur.)

SR2 requires that reactor systems have a very low likelihood and degree of core damage from initiating events. SR1 focuses on those aspects of reactor design and safety architecture which minimize the probability of accident initiating events occurring. The SR2 evaluations analyze system attributes that affect the probability that such SR1 initiating events could lead to core damage and the potential for designers to predict this probability correctly.

Three key sources of uncertainty are embedded in selecting the probability distribution functions for the SR2 criteria (these uncertainties also apply to SR3):

1. The completeness with which the system design and the requirements and implementation for its construction, operation and maintenance are known. Even after detailed design and construction is finished, some uncertainty remains in the actual configuration of a plant. Quality assurance activities during design and construction are used to bound these uncertainties.

2. The completeness of the identification of transient and accident scenarios to be included or excluded, and the accuracy of the assessment of their probability (SR1).

3. The ability to predict the transient response of the design to a given transient or accident scenario, and to correctly quantify the uncertainty in that prediction and the margin to core damage (or for other facilities, to criticality or to the release of radioactive material from its most immediate confinement).

For a given concept, some component of these uncertainties will be reduced with R&D, and some component will remain irreducible. Several of the SR R&D areas can contribute to increasing safety margins and reducing uncertainty in their prediction. The licensing and regulatory framework generate important feedback to the design, construction, and operation of facilities. Instrumentation and control systems, as well as human-machine interface issues, provide an area of large opportunity to reduce uncertainty in the prediction of plant response to transients. Reactor physics and thermal hydraulics modeling is key to predicting the transient evolution of accidents. Plant operation actions under accident conditions can likewise play a substantial role in affecting accident transients and uncertainty in their transient progression.

4. SAFETY AND RELIABILITY (GOAL 3)

Goal Statement:

Safety and Reliability-3 (SR3). Generation IV nuclear energy systems will eliminate the need for offsite emergency response.

Goal SR3 considers system attributes that allow demonstration, with high confidence, that the radioactive release from any scenario results in doses that have only insignificant public health consequences. Such confidence must come from the knowledge that reactor core damage (Design Extension Conditions, DEC, as described in the above introduction to "Criteria and Metrics for Safety and Reliability Goals") has very low probability (SR1 and SR2), and that mitigation features provide additional lines of defense to account for any significant residual risk. The objective of eliminating the need for offsite emergency response requires that we develop a high degree of confidence in our assessment of:

- The accuracy of the bounding prediction of the magnitude and timing of the radioactive source term and energy releases;
- The accuracy of the assessment of the effectiveness of the confinement system in accommodating energy releases and providing holdup of radioactive material; and,
- The resulting offsite dose probability distribution and comparison against appropriate standards for individual and societal risk.

An accurate assessment of the magnitude and timing of the source term must evaluate characteristics that minimize or delay the release, and the energy sources that can provide a driving force for the release. Features that minimize the source term such as fuels that are particularly robust to damage at high temperatures, coolants that chemically absorb released radionuclides, and thermal inertia that delays fuel damage progression must be demonstrated. Features that avoid or minimize potential energy releases under severe plant conditions must also be shown. Minimizing the potential for combustion of core materials, core materials interactions with coolant or structural materials depressurization events, formation of explosive gases, and potential for recriticality provides greater confidence in the bounding analysis.

Inherent or engineered features that mitigate fission product release provide additional barriers to the release of radioactive aerosols or gaseous fission products. . These barriers and mitigation features need to be robust to challenges from both internal and external events and should eliminate the potential for bypass of the mitigation systems or fission product barriers.

The assessment of the transport of radioactive materials in the environment, the estimation of dose and the evaluation of the associated health effects must also be performed with validated tools that assure confidence in the results and the comparisons with applicable safety guidelines and standards. Radiation transport and dose assessment tools must therefore include sufficiently general models and data bases for meteorological, chemical, and aerosol behavior to envelope the range of source term conditions that could be envisioned from Generation IV systems.

Appendix A

Licensing and Regulatory Framework

Appendix A

Licensing and Regulatory Framework

1. General Approach to Safety Assessments for Generation IV Systems

As for all of the current nuclear installations, Generation IV systems will meet safety objectives by implementing safety related architectures that can achieve, for all the plant transients and accidents identified by probabilistic safety analysis (PSA), the following fundamental safety objectives:

- Confinement of all potentially hazardous radionuclides
- Reactivity control for the fissile material
- Heat removal from the different heat sources.

To meet these objectives, Generation IV systems will introduce substantial innovative technological changes compared to current plants. These changes must be accommodated within a framework for licensing and regulation approaches; for example, the transition from prescriptive to performances based and risk informed regulations.

Risk informed should be part of an integrated decision making process that includes the need to[1]:

- Comply with the current regulations
- Maintain the defense-in-depth approach
- Provide for adequate safety margins
- Demonstrate risk reduction, risk neutral, or a small increase in the risk measures
- Monitor subsequent performance.

By merging the deterministic and the probabilistic (PSA based) approaches and results, this strategy can play an important role in developing the future Generation IV systems, supporting and justifying the predicted increase of the integrated plant safety, and simultaneously reducing costs. The safety related architecture will be simplified and the requirements for safety classification of safety systems and components will be reduced.

2. Defense-In-Depth Strategies

Defense-in-depth is generally structured in five levels; should one level fail, the subsequent level comes into play. Table 1-1 summarizes the objectives of each level and the corresponding means for achieving it.[2] The objective is to ensure that a single failure—equipment or human—at one level (and even combinations of failures) would not propagate to jeopardize the defense in subsequent levels. The independence of different levels is a key element.

Table A-1. Levels of defense-in-depth (From IAEA INSAG-10).

Levels of defense	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Offsite emergency response

A proposed method [3] for determining what requirements are currently applied to existing plants, should also be applied to Generation IV plants (see Figure 1-1).

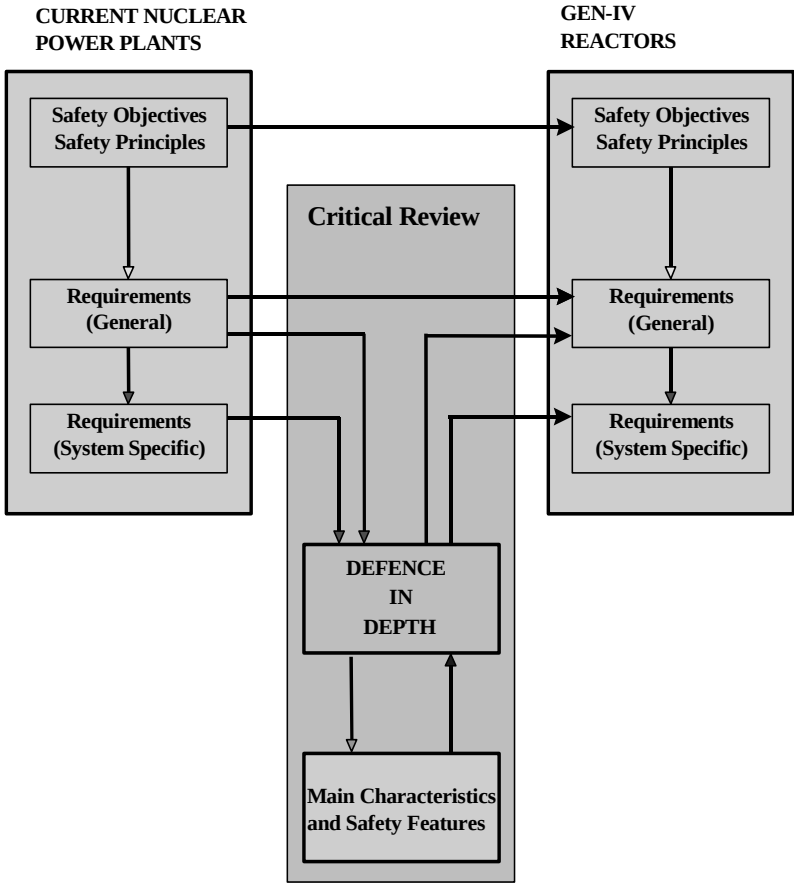

Figure A-1. Generation of requirements for Generation IV.

3. Challenges and Research Areas

Various new research areas involving licensing and regulatory issues are common to many of the Generation IV concepts studied, including some of those selected for near-term consideration.

3.1 Application of PSA and Deterministic Methods[1]

Because of the extensive use of passive components, the safety assessments of most of the Generation IV reactors focus primarily on initiating events of very low probability, such as structural failures due to extremely rare external events. The consequences of these events are determined by the direct phenomenological response of the plant to these events, rather than by a sequence of failures of systems that individually have higher probabilities, and which can be analysed and modelled with much less uncertainty. This aspect will pose significant challenges for the development and application of PSA methodologies to address these concepts, as explained further.

Traditional PSAs of LWRs consider sets of postulated initiating events, and follow them to various conclusions, resulting either in a successful termination of the transient (event) or in an accident state. The outcome will typically depend on the functioning of a series of actions by engineered safety systems or functions and/or operator actions. There is typically statistically useful data on the reliability of the components and systems involved, because failures are sufficiently frequent so that statistically useful failure probabilities can be estimated, and the functioning (or not) of the mitigating systems can be calculated with a credible uncertainty band. In addition, it is likely necessary to consider much longer mission times for passive components, such as several days compared to usual time of 24 hours.

Following the above arguments, various deliverables of this research would be the means for determining and quantifying the reliability of passive systems, particularly in the wake of extreme postulated initiating events (very specific environmental conditions), when they are most needed.

3.2 Definitions and Classification of Safety-Related Systems

Following the risk informed approach, system and equipment classification (safety grades), and more generally, the classification for all of the lines of defense, will be determined on the basis of their importance to the safety of the reactor. This will facilitate the optimization of the integrated safety related architecture and contribute to improvement of the integrated plant safety as well as to the plant economic competitiveness. To do this, each line of defense should be assessed both from performance and reliability view points.

Once more, the assessment of the performances of passive components or inherent characteristics will need specific methods and likely, further developments due to the unique characteristics that affect their predicted reliability. These needs will be established on a case-by-case basis.

3.3 Events to Be Considered for the Safety Assessment

An interesting aspect of the definitions question is how to categorize “design basis” and “severe” accidents for reactors that have as their objective the virtual elimination of accidents with any serious radiological consequences. The consensus could be achieved through a process that is coherent with the current practice, if the following recommendations are taken into account:

- For future designs, accidents beyond the “classical” deterministic design basis such as severe plant conditions, have to be considered at an early stage of the design to obtain a significant reduction of core damage frequency. Accident situations that would lead to large releases have to be eliminated

by design or " practically eliminated ." For example, if requested, the core melting for a given concept can enter within this logic and be eliminated by design or "practically eliminated."

- The accident scenarios to be considered for these demonstrations should be all those that can be judged as physically plausible. The process of selection of these scenarios should be based on deterministic analyses, supported, where needed, by probabilistic considerations, and engineering judgment. Accident scenarios need to consider reasonable potential human factors inputs that could remove a plant from its design basis operating condition.

- The accident sequences should be considered as " practically eliminated " if sufficient preventive design and operation provisions are taken. Nevertheless it is recognized that there is a need to develop more detailed guidance to clearly establish when sufficient design and operation provisions have been taken to practically eliminate an accident sequence.

- The evaluation of the remaining severe plant conditions should be performed using a " best-estimate " approach together with a quantification of the uncertainties to determine, for representative scenarios, a spectrum of the possible outcomes.

- Coherently with the risk informed approach, systems and components that are provided only for severe plant conditions should not require the same conservative analysis and requirements that are necessary for those developed to cope with design basis accidents. Nevertheless, their performance should be evaluated and documented along with suitable testing strategies and possible failure modes. There should be a high confidence that necessary equipment will survive severe accident conditions for the period that it is needed to perform its intended function.

3.4 Containment and Emergency Planning

Some Generation IV designs involve unconventional containments (low-pressure, vented), and claim that no emergency (evacuation) planning is necessary beyond the site boundary. Given these peculiar characteristics, the whole plant safety assessment should nevertheless remain coherent with the recommendations indicated under Section 3.3.

3.5 Safety and Reliability Issues for High-Temperature Process Heat Reactors

Some of the Generation IV designs have high-temperature capabilities and are being considered for applications such as hydrogen production, where joint-response safety considerations will be of considerable interest.

R&D is recommended to address the integrated safety requirements of a nuclear source with a hydrogen production plant. This will require close interaction with the chemical and refining industries.

As the requirements for other energy products and applications are more specifically defined, further crosscut issues will emerge. It is recognized that additional R&D may be needed to address these emerging needs.

REFERENCES

1. F. Niehaus, IAEA; T. Szikszai, IAEA, “Risk Informed Decision Making 2001,” INFCN-82, Topical 1.

2. International Nuclear Safety Advisory Group, “Defense-in-depth in Nuclear Safety,” INSAG-10, IAEA, Vienna, 1996.

3. Gasparini, M., “The IAEA Safety Standards for the Design. Application to Small and Medium Size Reactors,” *Seminar on Small and Medium Size Reactors, Cairo, May 2001*.

Appendix B

Radionuclide Transport and Dose Assessment

Appendix B

Radionuclide Transport and Dose Assessment

Safety and Reliability goals for Generation IV systems include minimizing both the likelihood and consequences of severe plant conditions, to the extent that offsite emergency response would not be required. In order to assess the potential for candidate Generation IV systems to meet that goal, a comprehensive analysis must be completed that includes initiating event probabilities, accident progression phenomenology, the associated radiological source terms and timing, and the subsequent radionuclide transport and dose assessment. Most stages of this analysis are plant specific and may therefore require new or improved tools to analyze new Generation IV system implications. The final stages of radionuclide transport in the environment and the resulting biological dose, are, however, more generic with the results depending primarily on the environmental assumptions and conditions, and the specific source term defined in earlier stages.

The RSCG reviewed current methods to assess whether Generation IV systems would require new methods or approaches to evaluate the transport and dose implications of severe plant conditions in these advanced systems. Generation IV systems will likely have different source term timing, aerosol characteristics or chemical compositions than current LWRs and could therefore require additional research to ensure that these models are sufficient to adequately address the implications of Generation IV characteristics for radiation transport and dose assessment. Improved phenomenological and real-time transport and dose modeling methods and models would support improved real-time emergency response, as well as optimized emergency planning methods and requirements.

Our general conclusion is that although Generation IV systems should not require fundamentally new methods to assess radiation transport and dose, there are areas where current analysis approaches may require refinement, or where current tools could be improved to support improved real time emergency response and emergency planning. These improved methods and models should be generally consistent with current approaches for radiation transport and dose assessment.

The RSCG focused on improvements in current transport and dose assessment methods that would support improved real time response or emergency management. These suggested areas for improvements would provide more accurate best estimate results that would be very beneficial in Generation IV analyses, but are not sufficiently fundamental that they would be essential from a viability perspective. This Appendix reviews the current methodology, highlights some of the limitations, and identifies some areas where improvements have been suggested.

1. Radionuclide Transport and Consequence Analysis Methodology

1.1 Current Analysis Methods/Approach

The analysis of radionuclide transport and the assessment of dose implications following a severe accident starts with a source term developed from either a severe accident analysis or a defined bounding analysis. The source term defines the magnitude, timing, chemical form, and aerosol characteristics of the radioactive release. Current models generally use basic meteorological, plume, aerosol, and health models to define dose and health implications to the surrounding areas. The current analyses of consequences are considered relative to safety goals, which generally consider prompt and latent cancer fatalities. Other consequences such as latent injuries or land contamination can also be estimated using current codes. This relatively straightforward approach used in current models is considered adequate since these analyses are

often carried out as bounding or conservative estimates to allow for the inherent uncertainties in defining accident conditions.

Current models and source terms obviously have been developed with a focus on LWR systems. The analysis approaches however, are potentially applicable to any nuclear power system with the appropriate definitions of source terms. This assumes that the databases for chemical and aerosol phenomenology are sufficiently complete to provide a basis for the analysis of a the required range of source terms.

1.2 Representative Current Codes

Although there are several radiation transport and dose assessment tools that are available, one of the tools most commonly used by the NRC is MACCS2, which is representative of the current practice. MACCS2 is the NRC Level-3 PRA tool that is used for both commercial applications and by DOE facilities for authorization basis analyses. RASCAL (Radiological Assessment System for Consequence Analysis) is the NRC emergency response tool that provides real-time decision support in accident management for predicting dose to populations. There are many other U.S. codes that provide similar functionality to these two codes, some of which provide more sophisticated models.

MACCS2 uses a simple Gaussian plume model. As such, plumes travel in a straight line rather than following transient wind directions. Some other codes are based on Gaussian puff models, which do allow plumes to follow transient wind directions. Health effects and economic consequence models in MACCS2 are generally basic. MACCS2 does not model surface relief effects, which are considered important by some.

RASCAL and subsequent models, and some other codes are capable of real-time simulations. RASCAL models include reactor source term, atmospheric transport and doses resulting from radiological emergencies. RASCAL was developed for the U.S. NRC and is designed to be used in the independent assessment of dose projections during response to radiological emergencies. The code provides a comparison to EPA Protective Action Guidance and thresholds for acute health effects. RASCAL computes power reactor source terms, airborne transport of activity (through both Gaussian plume and puff models), and the resulting doses. The results allow easy comparison to EPA protective action guidelines

2. Generation IV Reactor Characteristics

2.1 Generation IV Reactor Severe Accident Considerations

Next generation nuclear power systems under consideration include advanced water cooled, high temperature gas cooled with graphite based fuels, liquid-metal cooled systems and a range of other systems that have significantly different characteristics from a current LWR. These systems potentially have severe accident sequences and characteristics that involve different temperatures, timing, energy release considerations, aerosol characteristics, and chemistry that may affect transport and dose assessment. Safety analyses for these systems result in characteristic source terms that may have different quantitative and qualitative characteristics. Generation IV reactor analysis must develop accident sequences and source terms that are comprehensive for that system. These source terms may have significantly different characteristics, such as in chemical or aerosol models, that must be accounted for. Nevertheless, improved models and tools should account for these differences. The Generation IV source terms, however, do not appear to require fundamentally new approaches, such as new atmospheric dispersion models. Current code approaches like MACCS2 should be applicable to a Generation IV reactor with the appropriate consideration of phenomenology and database.

2.2 Generation IV Source Term Characteristics

Improvements in the currently available radiation transport and dose models would be driven by the characteristics of the advanced reactor source terms. Advanced reactors could potentially involve sodium or graphite oxidation as a source term generation and initial release consideration. The chemical form of the released fission products and the aerosol particle size would be affected by these accident initiators. Designs that involve very high burn-ups or fuel recycle, would also have fission product distributions, timing, chemical forms, particles size distributions that may affect transport or dose assessment. Establishing the appropriate source term for these advanced systems would appear to be the more fundamental requirement to adequately assess transport and dose implications of these systems. NRC is already funding work to modify MELCOR to analyze Generation IV reactor source terms.

3. Radionuclide Transport Considerations

MACCS2 uses a simple Gaussian plume model. As such, plumes travel in a straight line rather than following transient wind directions. More sophisticated models are available, and MACCS2 and similar codes can be improved with the inclusion of Gaussian puff models, which do allow plumes to follow transient wind directions. Health effects and economic consequence models in MACCS2 are generally basic and, although improvements are possible, the benefits should not be unique to Generation IV systems. MACCS2 does not model surface relief effects, a quality considered important by some. Surface relief effects are probably much more important for real-time modeling than for PRA-type modeling. The NRC is considering providing improvements in some of these areas.

Some areas where improvements or more sophisticated models would be beneficial for future systems include (a) plume models to allow more realistic transport in transient conditions, and (b) validated models for aerosol and fission product chemistry effects for the range of Generation IV systems (gas, Pb-Bi, Na coolants, high burn-ups, etc.). Improved methods and more sophisticated phenomenological models would provide more robust analyses, and increase confidence in results used as the basis for improved emergency planning and response for Generation IV systems.

4. Dose Consequence Considerations

4.1 Biological Interaction, Food Chain

The presence of different core or coolant materials (C, Na, Pb, etc), higher temperature releases, higher burn-up, or recycle compositions could affect the chemistry of some fission product elements and compositions, and therefore, affect doses to humans through inhalation and food chains. Food-chain parameters are input to MACCS2 and other similar codes. Although the basic models would probably not have to be changed, the input parameters that determine reaction chemistry would need to be revised if chemical forms are different.

4.2 Biologically Important Nuclides

Generation IV systems would be expected to have generally longer burn-ups, have different fission product inventories based on the core thermal power, have different core and coolant materials, and eventually utilize recycle fuel cycles that could lead to a somewhat different distribution of fission products and other activated materials. Although the proportions might be different, the list of biologically important fission product nuclides would be nearly the same. Systems with Pb-Bi coolants, or graphite cores would add activation products that may have to be considered.

5. Summary

Improved phenomenological and real-time transport and dose modeling methods would support improved real-time emergency response, as well as optimized emergency planning methods and requirements. The differences in system characteristics of Generation IV systems should not require fundamentally new methods to assess radiation transport and dose. Generation IV systems will have different source term timing, aerosol characteristics, or chemical compositions that will require additional research to adequately define the source term. The methodology to transport and evaluate dose implications, however, should look similar to the current approaches and improvements should fit within the current framework.

Appendix C

Instrumentation and Control and the Human-Machine Interface

Appendix C

Instrumentation and Control and the Human-Machine Interface

The purpose of this section is to identify crosscutting instrumentation and control (I&C) and the human-machine interface (HMI) research and development initiatives that would address the risk and safety of the selected Generation IV reactor concepts. These topics are restricted to those R&D efforts that would apply to reactor concepts in two or more TWGs, and those that would not be pursued (probably with greater support and resources) by other established industries over the next decade or so.

The Generation IV I&C area has some natural overlap with operations and maintenance (O&M), (Appendix F) and with Human Factors (Appendix G). Human factor considerations for the modular Generation IV plants would require significant R&D to adapt to the idea of having many small units controlled from a single control room (with "fewer-than-normal" operators per unit). However, due to the Generation IV passive safety characteristics goals, operator action (or misaction) is by design not supposed to be safety-significant. Hence it could be argued to belong in the O&M category. The I&C/HMI area also supports Licensing and Regulatory Framework (Appendix A), Radionuclide Transport and Dose Assessment (Appendix B), and Reactor Physics and Thermal Hydraulics (Appendix D). It is also an integral part of Risk Management (Appendix E).

1. Sensor Development and Related R&D Areas

Sensor development, as it would apply to the risk and safety area, would be likely to focus on extending the temperature range (upward), since higher temperatures are generally necessary to attain the Generation IV goal of higher efficiency. For the six concepts selected by GRINS, this area would apply primarily to the two gas reactor concepts (VHTR and GFR in TWG-2), but there may be applications to future upgrades of several concepts from other TWGs such as the MSR.

For safety robustness, high reliability, testability, "smarts," and redundancy are also needed. Where applicable, resistance to radiation needs to be factored into the design and testing, and would also need to be taken into account the Generation IV goal of higher burn-ups.

On the other hand, for the passively-safe Generation IV designs, many measurements that previously (Gen-II or -III) required a safety-grade status may no longer be needed for "safe shutdown." Because of the longer (Generation IV) time delays in the reactors' critical response to accident conditions, fast response times for the sensors are not as crucial. The safety grade requirements issue should be closely tied to "Licensing and Regulatory" topics (Appendix A).

With regard to crosscutting attributes, sensor requirements for the various TWG concepts would typically differ greatly depending on the primary coolant; however, some forms of in-core detectors could apply to many different concepts. For this, R&D support for initiatives such as high-temperature, durable self-powered neutron detectors, perhaps with other built-in parameter measurements such as temperature, would be beneficial and certainly unique to the reactor industry.

Other more generic sensor-related R&D need possibilities could include diagnostic systems for startup and post-shutdown, as well as special monitoring for post-accident assessments. The Generation IV goal of not requiring offsite sheltering and evacuation planning implies that reliable post-accident monitoring and diagnostics would be desirable to ensure that no special offsite actions are in fact

required. Post-accident instrumentation (environmental measurements and diagnostics) would also have many elements in common with non-nuclear processes and systems, such as chemical and biological.

2. Human-Machine Interface Issues

Along with I&C, the HMI issues have been too often relegated to the final stages of the design process: HMI is the applied glue that allows the selected system design to function in the real world. Such after-the-fact design can lead to situations where the lack of foresight with respect to the full range of interactions can create cognitively challenging situations where the control systems and the operators have difficulty responding properly.[1,2,4] It is useful to think of the plant/I&C/HMI/operator "system." This combination must be well designed as a single entity if safety and reliability are to be optimized. In particular, human factors considerations, which should be integrated into the earliest stages of design, are sufficiently important that they are discussed in greater detail in a separate Appendix.

Generation IV concepts should begin to integrate I&C and HMI in the viability evaluation stage. At this time it appears that most crosscutting I&C and human factors research and development initiatives that address the risk and safety of Generation IV reactor concepts would benefit all concepts, rather than discriminate among them. Although, in some cases, R&D on particular prognostics could possibly alleviate safety concerns associated with particular chemistry, materials, and physics issues in particular designs, thereby removing problems that could have eliminated a concept. In addition, many I&C R&D efforts are likely to be supported by other established industries over the next decade or so. Such efforts will be identified here to permit tracking them to ensure that they do move forward.

I&C is related both to the physics design of the facility and to the interactions between the physical machine and its software and the human operators and maintenance staff. Specification of the I&C/HMI includes physical requirements and human requirements. Thus, the HMI needs more than the reactors designer's viewpoint, it also requires specification of the human factors needs. The evaluation must be aware of the trade-offs between efficient process control and upset identification and control, between optimal facility response when the I&C works perfectly and under all failure modes, between fast-acting control systems and human understanding and control, and between production and safety. Trevor Kletz has documented many cases of advanced control systems problems and failures and their impacts on the human operators.[3] Finally, the emphasis, from a safety point of view must focus on the unexpected. We can be assured that designs will be well protected against expected conditions, including upset. The real dangers come from unexpected conditions and actions. Successful "systems" must be flexible enough to provide safe options when the unexpected occurs.[5]

There are two other specific systems or components for which generic (crosscutting) safety-related I&C R&D would apply, and more may be identified as Generation IV research progresses. These are the Reactor Cavity Cooling System (RCCS) monitoring, and I&C related research that would improve the safety basis for the Coated Fuel Particle (CFP).

3. Reactor Cavity Cooling System Performance Monitoring

The RCCS is common to both the gas-cooled (VHTR, GFR, and the PBMR, GT-MHR, etc.) and liquid-metal cooled Generation IV reactors. The AHTR (TWG-4) also requires an RCCS. In the gas-cooled designs, at least, it is considered safety-grade, representing the final and necessary heat sink should all else fail. The monitoring of various modes of passive RCCS designs, including performance validation, on-line testing, and degradation analysis, is challenging due to the large size and passive-cooling attributes. Some concerns about RCCS performance that should be monitored and analyzed are heat transfer degradation (fouling, lowered emissivity, etc.) and leaks. Since the RCCS operates all the

time, there is the dual requirement to minimize heat removal during normal operation (parasitic loss), and provide adequate heat removal for accident conditions.

4. Coated Fuel Particle I&C for Quality Assurance/Quality Control

Although "I&C for the CFP" would not normally be regarded as "reactor I&C," it is included here to emphasize the CFP's important safety role for the gas-cooled reactors (PBMR, GT-MHR – TWG-2) and the AHTR (TWG-4). The "TRISO" CFP is the initial and primary barrier between the fuel kernel with its fission products and the primary coolant. The I&C challenge is that there are a billion or so tiny (1 mm diameter) CFPs in a typical core, each responsible for containing its fission products for both normal and accident conditions. Very low failure rates and percentages are required, particularly when the design incorporates a vented containment. As a result, there would be a great incentive to have excellent control over the manufacture and testing of each CFP. Currently, the manufacture and Quality Assurance/Quality Control involve fluidized bed (chaotic) coating processes for the TRISO protective layers, and statistical testing of the resulting batches of CFPs. Since the ceramic CFP is currently the only nuclear fuel form capable of supporting the high reactor temperatures needed for advanced process heat applications, generic R&D for "crosscutting" I&C needed for manufacturing and testing is justified.

References

1. S. Dekker, *The Field Guide to Human Error Investigations*, Ashgate, Burlington, 2002.

2. E. Hollnagel, *Cognitive Reliability and Error Analysis Method: CREAM*, Elsevier, New York, 1998.

3. T. Kletz, *Computer Control and Human Error*, Gulf Publishing Co., Houston, 1995.

4. J. Reason, *Managing the Risks of Organizational Accidents*, Ashgate, Burlington, 1997.

5. K. E. Weick and K.M. Sutcliffe, *Managing the Unexpected: Assuring High Performance in an Age of Complexity*, Jossey-Bass, San Francisco, 2001.

Appendix D

Reactor Physics and Thermal Hydraulics

Appendix D

Reactor Physics and Thermal Hydraulics

Design and optimization for safety and reliability requires the ability to identify and quantify the probability of potential transients and accidents, to predict the resulting response of the nuclear energy facilities, and to quantify and bound the uncertainty in these predictions. The ability to model reactor physics and thermal hydraulics plays a key role in bounding the range of possible initial system states, and predicting the subsequent transient response. These analyses focus on predicting the value of key system parameters, such as peak fuel temperature, achieved during a transient, and comparing them to a defined threshold where damage or some other negative outcome would be expected to occur. The difference between the predicted peak value and the threshold is referred to as margin, and the ability to quantify margins and their uncertainty is a key goal for reactor physics and thermal hydraulics analysis.

Uncertainty comes from a variety of sources, which require systematic approaches to identify and bound the effects that come from incomplete knowledge of them. One example of a source of uncertainty is uncertainty in the initial state of the system. This uncertainty arises from the potential for variation in the fabrication of components and construction of the facility, which is reduced by the application of quality assurance measures, and the activities of surveillance, operations, and maintenance, which are governed by facility technical specifications. Reactor physics and thermal hydraulics experiments and models are then used to predict subsequent transient response for a defined system initial state, or range of initial states, and initiating event.

Formal methods for predicting transient response and quantifying uncertainty include the Code Scaling, Applicability and Uncertainty (CSAU) methodology[1] adopted for reactor licensing in the United States. This method allows core-damage parameters such as peak fuel or clad temperature to be estimated and compared to prescribed acceptance limits. CSAU uses computer codes to model the reactor response to potential transients and accidents. The uncertainty in the code prediction of the plant response comes from two primary sources[1]: plant operating conditions and process variables that arise from imprecise knowledge about the reactor state during the transient; and code, scale, and experimental contributors.

Reactor transient response is governed by a wide range of transport phenomena. Some of these phenomena have substantially stronger effects than others. CSAU uses a Phenomena Identification and Ranking Table, that subdivides the transient processes into spatial regions and temporal periods where they occur, which allows identification and ranking of all phenomena using scaling analysis and expert assessment. The capability of the code to model the high-ranked, dominant phenomena is then confirmed from the code documentation. If the code cannot adequately model the phenomena, expert assessment is used to determine a bias to be applied to the code results. Codes for Generation IV plants will be expected to model all dominant phenomena to minimize the need for and uncertainties from this expert assessment.

Reactor safety codes nodalize reactor systems into discrete control volumes and evaluate transient processes using finite time-step sizes. This introduces numerical errors, in particular from artificial diffusion effects that depend on the size of the control volumes used. These errors can be assessed using grid and time-step refinement studies. The CSAU method identifies an appropriate nodalization for a reactor system, and then requires that this nodalization be used consistently throughout the evaluation process.

Because conserved quantities are averaged over control volumes, the information lost by averaging must be replaced using constitutive relationships to predict parameters such as heat transfer coefficients and friction factors. The contributions of these constitutive relationships to code uncertainty are quantified

using a statistical comparison of code results with separate-effects experimental data. Where the experimental data base is not sufficient to adequately characterize the probability distribution and bias, expert assessment is used to estimate a conservative probability distribution or bias. Expert assessment is also used to estimate bias when extrapolations in scale are required between available experimental data and the conditions to be modeled. Generation IV reactor analysis will be supported by well-scaled and instrumented experiments and physically based models for dominant phenomena, to minimize the uncertainties introduced by this type of expert assessment. Because many fundamental transport phenomena, such as convective heat transfer, are shared by many Generation IV concepts, research to improve the ability to model these phenomena will crosscut these concepts.

Once uncertainties in constitutive relationships are characterized, sensitivity studies are employed to assess the total code uncertainty. Integral experiments provide independent verification of the capability of the reactor safety code to model integrated system response and confirm that no key phenomena or processes have been missed in the code development effort. It is impractical to study all combinations of parameters experimentally, so integral experiments play a confirmatory role. Furthermore, it is anticipated that evaluations will occur before prototype-scale integral experiment test results would be available. Expert assessment of code results is used to judge the effects of the extrapolations of scale and parameter values away from the integral experiment database. For Generation IV reactor licensing, integral code validation will be provided by well-designed experiments with minimal scaling distortion, and preferably by experiments performed directly in a full-scale prototype plant.

The following specific areas of modeling crosscut multiple concepts.

1. Physical Modeling

Physical modelling of energy and mass transport includes:

- Single and multiphase flows:
  - multicomponents
  - phase change formulation
  - flow regime
  - effect of large voiding
  - critical flow.

- Transient heat and mass transfer:
  - convection
  - conduction
  - radiation
  - phase change.

- Material descriptions:
  - equation of state, interfacial area, velocity fields
  - transient state and innovative material modelling
  - material interaction.

Physical modeling of neutronics includes:

- Transport equation, neutronics libraries.
- Converged solution under complex fuel configurations.

- Strong and continued coupling between power and material temperature/motion.

2. Numerical Methods

The numerical method of discretisation includes:

- Numerical method and solution for conservation equations with multi-component/multi-phase flow
- Reliability
- Robustness/rapid transient with phase change or without phase change
- Robustness/void fraction
- Mass balance/energy balance
- Low CPU cost.

The numerical method of uncertainty studies includes:

- Numerical diffusion
- Sensitivity studies.

3. Qualification

- Phenomena identification and ranking.
- Comparison to other codes with different time-integration scheme (explicit to implicit).
- Analysis of qualification tests and experiments:
    - separated effect experiments:
        - variety of initial and boundary conditions
        - simulant materials
        - scaled geometries.
    - integral experiments:
        - design and scaling.
- Neutronics benchmarks.

Appendix E

Risk Management

Appendix E

Risk Management

Risk Management brings all the SR issues together. The approach for evaluating and controlling risk in Generation IV systems needs to extend the popular view of PRA in several directions. Whether this amounts to crosscutting R&D or simply application of known principles is open to debate. There is no doubt that organizing these concepts into a clear approach that can be used by researchers and evaluators in a practical way will require significant effort.

We begin with a general framework for analysis of risk in Figure E-1. (To some, this is simply what PRA is; to others, it is a far cry from the set of event trees and fault trees they call PRA.)

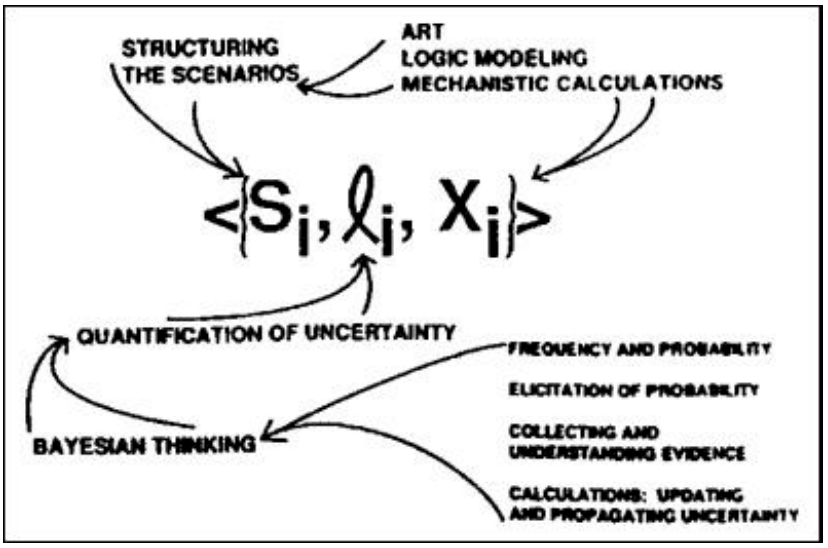

Figure E-1. General framework (language) for risk analysis.

Conceptually risk analysis identifies a simple triplet:

S_i = the scenario (i.e., what can go wrong),

ℓ_i = the likelihood of the scenarios occurring, and

X_i = the consequences of the complete scenario

Then the risk analysis is the assembly of all possible such triplets. The art of risk analysis comes in structuring the search for scenarios, S_i, and in organizing the structure of the scenarios in a way that facilitates analysis. This can mean effectiveness of search, ease of calculation, clarity of presentation, etc. The science comes in the detailed analysis of the identified scenarios and their consequences. And tying it all together is the structure for identifying, quantifying, and explaining the uncertainty in the elements of the analysis.

It is important for the Generation IV Viability and Performance Evaluation phases to recognize that each of the elements of the triplet can be evaluated at alternative levels of detail. The following schema is a preliminary view of how such a step-wise progression of successive approximations to complete PRA detail could proceed. All cases fit the basic outline of Figure E-1.

Case 1. Qualitative criteria. Criteria such as the levels of defense-in-depth as discussed in INSAG 10, "Defense-in-depth in Nuclear Safety," and adopted in the Final Screening and R&D Prioritization criteria for the Generation IV roadmap, such as robust engineered safety features and system models that have small and well-characterized uncertainty. Later cases become more analytical and quantitative, but the basic principles of these qualitative criteria continue to apply.

Case 2. Initiating event/potential consequence evaluation. In this case, analysts apply a formal search process to identify possible initiating events (departures from normal steady-state operations). The search must go further than replicating initiating events identified in Generation II and III PRAs or standard design practice. To be effective, it requires an understanding of the consequences to be modeled later in the full PRA. Maximum potential consequences are assigned in a conservative manner to lend some sense of priority to the list, but lacking full event sequence development, cannot be taken literally. Such an examination provides the first input to later PRA development, often identifies potential new events, and thereby supplements the qualitative criteria of Case 1. A formal search process needs to be defined and tested, but will almost certainly borrow heavily from the HAZOP techniques of the chemical industry.

Case 3. Functional scenario development. One approach that has proved viable for a "first-look" PRA emphasizes a structured development of the detailed functional scenarios (the S_i of Figure 1) that can progress to damage states of interest. The design needs to have progressed to the point that the systems capable of providing key safety functions have been defined. Such scenarios can be developed in many forms: flow charts, narrative descriptions, event trees, etc., or the results of simulation. The important thing at this level is that they be complete—as close as possible to the scenarios that would be analyzed in a full quantitative PRA. Quantification of these scenarios may be crude at this time, but should allow for uncertainties due to random behavior and current state of knowledge. Major portions of a Case 3 PRA would depend on expert elicitation, bringing together the evidence (partially applicable data, experimental and experiential information, preliminary or complete calculations, etc; i.e., all available information. A formal definition of this approach should be developed and is expected to draw on available experience from similar studies, for example, the Seabrook Station and South Texas Project "Phase 1" PRAs from the mid-1980s, and similar studies performed for a number of chemical process plants at the turn of the century (1998–2002). One similar approach is documented in a recent book published by AIChE.[6]

Case 4. Full quantitative PRA. In the most thorough application of PRA, the design must be far enough along to identify component characteristics, points of possible (not just planned) human interaction, procedures and training, physical mechanisms that apply supported by mechanistic calculations, and experiments (physics, chemistry, corrosion processes, etc.). Even when full data are not available, there must be enough information available to support expert elicitation.[10] Even in a "full quantitative PRA," there are alternative levels of available information to support quantification; for example, success criteria and consequence results depend on the available detail in mechanistic calculations and experiments, on the available data on component performance in normal environments and highly stressed environments. Mechanistic calculations can run all the way from simple energy balances (these simple calculations can be useful to bracket a range of possible conditions that could occur in related scenarios) to the systematic consideration of uncertainty in the CSAU approach.[11] It is always necessary to apply judgment to such information and adapt what is available to what is needed; this transformation always results in uncertainty that needs to be considered in the analysis. The best form of the scenario structuring (event tree/fault tree models, simulation models, etc.), mechanistic analyses, and evaluation of likelihood (in Figure E-1) will depend on the scenarios themselves—the state of design information, and the quality and applicability of available information. It will be useful to develop defined, alternative approaches to support the Viability and Performance evaluations.

In the most common form of current PRA, the basic plant level scenarios (level 1 PRA) are structured by initiating events that couple to event tree sequences, which in turn are analyzed by fault trees (logic models of system success/failure) and "first generation" human reliability methods (HRA). Coremelt progression (level 2) scenarios are structured into event trees and post-release scenarios are structured by simulation models.

For Generation IV plants, with many passive systems, fault trees may be very simple when events proceed on expected trajectories. In such cases, it is possible that "Because of the extensive use of passive components, the safety of these reactors is determined by initiating events of very low probability, such as structural failures due to extremely rare external events. The consequences of these events are determined by the direct phenomenological response of the plant to these events, rather than by a sequence of failures of systems, which individually have higher probabilities and which can be analysed and modelled with much less uncertainty. This aspect will pose challenges for the use of PSA."[1]

Alternatively, the real work of PRA may lie in the search process for the scenarios. Clever ways to structure the search for unexpected conditions that can challenge design assumptions will need to be developed or identified and applied to these facilities. Rather than the very low probabilities envisioned above, the risk may arise from unexpected ways the facility can end up operating outside its design assumptions. For example, Reference 2 develops a HAZOP-related search scheme for scenarios that deviate from designers' expectations, while Reference 3 applies a structured search for construction errors. Other ways that the facility can end up operating outside its design assumptions could include scenarios (a) where the human operators and maintenance personnel place the facility in unexpected conditions, or (b) where gradual degradation has led to unobserved corrosion or fatigue or other physical condition far from that envisioned in the design

Weick has recently pointed out that the real key to safe operations is a focus on managing the "unexpected."[4] In fact, searching for the unexpected is exactly what PRA originally did. With repeated application to similar Generation-I and II plants, some analysts have lost sight of that. In a recent address at a USNRC colloquium,[5] the Director of Research indicated that in applying PRA to future reactor designs, analysts must start with a clean page—not be biased by expectations from the conclusions of PRAs on old designs.

To address these potential problem areas, a new way to look at human performance and HMI is needed. New "second generation" HRA methods focus on context and control,[7] on how the organization[8] and the plant state[2] can "set up" the operators for failure. The modern approach shifts the focus from human "error" as the cause of accidents to unsafe actions as a symptom of more systemic problems. The focus in both retrospective event investigation and in prospective HRA shifts to seeking understanding of why operators' actions were locally rational, that is, why what they did made sense at the time, given the context in which they were operating (as opposed to the hindsight of knowing how things turned out and how they might have progressed differently).[2,7,8,9] The methods for a new type of HRA go beyond standard task analysis and table lookup of average human error probabilities. They look for the triggers for desirable and undesirable human performance.

There is a need for Generation IV to develop a specification for needs of HRA. Then it will be possible to see if currently developing methods are sufficient or if further development is needed.

Closely interwoven with human performance are the I&C system and the HMI. Note that I&C systems alone cannot solve the problem; they must be matched to the human operators and maintenance personnel. Kletz[12] gives a number of example events showing how advanced digital control systems have failed in ways that proved cognitively challenging to operators, have not been well-matched to human capabilities, or have behaved strangely because of maintenance problems. However, if design of these

systems is well-matched to human abilities and, especially, to avoiding the kinds of cognitive problems identified by the new HRA approaches, Generation IV systems can avoid many of the difficulties that have faced operators in current facilities.

In addition to the human factor issue, I&C systems have the potential to permit better management of those problems discussed above that can erode the design assumptions for new plants. If such systems can provide prognostics to control plant (and operational) degradation before risk increases, PRA examination of such possibilities can be limited and we can have better confidence in system performance and PRA calculations.

References

1. IAEA Document on MHTGRs

2. M. Barriere, D. Bley, S. Cooper, J. Forester, A. Kolaczkowski, W. Luckas, G. Parry, A. Ramey-Smith, C. Thompson, D. Whitehead, and J. Wreathall, "Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)," NUREG-1624, Rev. 1, U.S. Nuclear Regulatory Commission, May 2000.

3. D. C. Bley, S. Kaplan, and D. H. Johnson, "The Strengths and Limitations of PSA: Where We Stand," *Reliability Engineering and Systems Safety*, vol. 38, 1992.

4. K. E. Weick, and K. M. Sutcliffe, *Managing the Unexpected: Assuring High Performance in an Age of Complexity*, Jossey-Bass, San Francisco, 2001.

5. USNRC RES Colloquium … May 2002.

6. *Layer of Protection Analysis: Simplified Process Risk Assessment*, CCPS, AIChE, 2001.

7. E. Hollnagel, *Cognitive Reliability and Error Analysis Method*: CREAM, Elsevier, New York, 1998.

8. J. Reason, *Managing the Risks of Organizational Accidents*, Ashgate, Burlington, 1997.

9. S. Dekker, *The Field Guide to Human Error Investigations*, Ashgate, Burlington, 2002.

10. R. J. Budnitz, G. Apostolakis, D. M. Boore, L. S. Cluff, K. J. Coppersmith, C. A. Cornell, and P. A. Morris, "Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts," NUREG/CR-6372, U.S. Nuclear Regulatory Commission, Washington, D.C., 1997.

11. B. E. Boyack et al., "An overview of the code scaling, applicability, and uncertainty evaluation methodology," Nuclear Engineering and Design, Vol. 119, pp. 1-16, 1990.

12. T. Kletz, *Computer Control and Human Error*, Gulf Publishing Co., Houston, 1995.

Appendix F

Operations and Maintenance

Appendix F

Operations and Maintenance

Three O&M areas have been identified to ensure reliability and safety of Generation IV systems in all operating modes (normal-operation, design-basis-accident, and severe-accident): advanced hardware (includes hardware for maintenance), advanced software/procedure for both operation and maintenance, and interface between advanced hardware and software. This Appendix covers the first two areas, the third, which involves R&D, is described in Appendix C.

Advanced Hardware

Some Generation IV hardware (components and systems) are exposed to more severe conditions than the hardware in present systems. For example, the coolant temperature in most Generation IV systems is higher than in current LWRs. Consequently, advanced components/systems are often unique, requiring new maintenance hardware. Two stages of R&D are generally recommended for such advanced hardware, including maintenance hardware: development of advanced components/systems, and confirmation of their reliability under various expected conditions.

Development

Optimization for advanced Generation IV hardware must consider reliability, operability, maintainability, and economics. Major development fields include:

- Materials, including surface treatments
- Structures
- Layout (arrangement)
- Manufacturing/installation methods.

Crosscut R&D

There are very few crosscut R&D areas because the design features of most Generation IV systems are unique. However, one feature that appears to crosscut Generation IV systems is a higher coolant temperature. R&D for this feature will involve developing:

- Structures to mitigate thermal stress, thermal shock, or thermal fatigue caused by high temperature (difference) coolants.
- Surface treatment materials for the structures confining the coolant.

Confirmation of Reliability Under Various Conditions

Historically, the reliability and operability of advanced O&M hardware has been confirmed by tests under various expected conditions (but not necessarily before their deployment). Major targets of these tests have been mechanical/structural integrity, system performances, including safety system responses, and the compatibility of advanced hardware with the other systems. Due to recent computer

technology improvements and experience accumulated from earlier systems with similar components, we may be able to substitute these confirmation tests with small-scale tests or computer modeling simulation.

Crosscut R&D

Some existing experimental test facilities can create irradiation, seismic, and severe environmental conditions or other test environments. We may be able to share these facilities to conduct R&D on some Generation IV systems. Measurement and computer simulation tools might also be shared to evaluate mechanical/structural integrity and system performance, including safety system responses.

Mechanical/Structural Integrity

Environmental qualification (EQ) tests of the advanced hardware used in Generation IV systems have been carried out before they are used for the newly developed nuclear plants. Other than typical EQ tests, the mechanical/structural integrity is confirmed after considering the following items.

- Irradiation, thermal creep such as reactor internals
- Seismic influences such as control rod mechanical response under seismic condition
- Corrosion influences such as on valves under high-temperature coolant conditions
- Erosion influences such as on turbine blades
- Flow induced vibration (FIV), fretting influences such as on fuel rods in flow
- Thermal cycle, stress, and insulation such as in reactor vessel nozzles
- Aging, etc., such as in seals, bearings.

Performance Confirmation for Nonsafety Systems

To confirm effective performance of the advanced hardware, iterative tests are generally carried out under various conditions. The results are often used as input for probabilistic safety analysis (PSA).

Performance:

- Startup characteristics, such as emergency power sources
- Rated performance characteristics such as valve opening time.

Conditions:

- Normal conditions
- Seismic conditions
- Design basis accident conditions
- SA conditions.

Safety Related System Responses at Various Initiating Events

Demonstration tests are generally carried out for various initiating events to confirm reliability of safety related systems. The identification of initiating events is also an R&D item for Generation IV systems. These experimental results are often used for PSA.

Initiating events:

- Identification of initiating events
- Design basis accidents (DBA) such as loss of coolant and loss of flow
- Reactivity insertion accidents (RIA) such as control rod withdrawal
- Severe accidents (SA) such as core damage.

Compatibility with the Other Systems

Compatibility among the systems is being investigated in this stage of R&D. In particular, the adoption of the advanced hardware and safety systems sometimes result in large design changes to building structures, such as passive safety systems and maintenance hardware integrated with buildings.

Advanced Software/Procedure

A higher level of reliability and safety is achieved not only by hardware, but also by software and procedures for O&M. Two areas that could benefit future Generation IV systems are the development of advanced O&M procedures and verification of advanced O&M procedures.

Development of Advanced O&M Procedures

New O&M procedures will need to be developed because the Generation IV systems use unique hardware and are operated under unique conditions. New plant parameters that must be controlled for operation will need to be identified because the plant parameters (pressure, temperature, flow rate, etc) of Generation IV systems are also unique. The followings are examples of R&D for such advanced O&M procedures.

- Plant parameters to be controlled
- Plant parameter control systems and monitoring systems
- Automatic startup/operation/shutdown systems and procedures
- Refueling machines, control rod uncoupling mechanisms, and procedures
- Pump maintenance machines, vessel inspection machines, and procedures
- On-line/remote maintenance systems and procedures
- Maintenance-free systems/components.

Sensors and signal transmitters (electric cables, etc.) for most monitoring tools are sensitive to environmental conditions such as radiation and temperature. Consequently, the existing tools may not be optimal for Generation IV systems. New reliable monitoring tools will need to be developed for Generation IV systems, and their reliability under various conditions verified.

Crosscut R&D

R&D of control and monitoring systems might be crosscut areas for Generation IV systems. These areas are described in Appendix C.

Verification of Advanced O&M Procedure

O&M procedures are usually verified using plant simulators or mockup tests. Therefore, Generation IV simulators must be developed before detailed O&M procedures. These simulators can generate valuable feedback for operations procedures and components/systems designs. Such simulators are also critical for operator training, and can also benefit public relations.

For example, for LWRs a scram is initiated by logic sets based on multiple operating parameters. As mentioned in the section above, some Generation IV systems will monitor plant parameters much different from those for current LWRs. Operating conditions and components/systems responses for the Generation IV systems will be substantially different from those in LWRs. Those differences create R&D needs for hardware/software logic for normal operation, as well as accident conditions for Generation IV systems.

Mockup tests for LWR maintenance procedures are commonly used for maintenance activities such as pump maintenance and coupling/uncoupling of control rods with drive mechanisms. They are also useful in worker training to help reduce the time required for maintenance and to lower worker radiation doses and increase plant availability.

Crosscut R&D

R&D for plant simulators have some common areas for all the Generation IV systems, but mockup tests are unique to individual designs.

Appendix G

Human Factors

Appendix G
Human Factors

To maintain the competitiveness and public acceptance of nuclear power, and to achieve Safety and Reliability (SR) Goal 3, Generation IV nuclear energy systems will comply with stronger safety and productivity goals than the systems presently in operation. The achievement of these more ambitious goals will require systematic consideration of human performance as a major contributor (positive or negative) to plant operation efficiency and safety, as well as relying on technical improvements. This also requires the identification of favorable conditions for the human intervention in the plant, for central control room tasks, and for field operations such as maintenance, periodic testing, etc.

The importance of identifying and optimizing human factors requirements in the design of future nuclear power plants is now an idea commonly accepted and put forward by the design community, but often with an important flaw. Generally, human factor issues are only considered during the later phases of facility design when, in the best case, instrumentation and controls (I&C) are designed using such things as human-centered automation approaches, or in the worst case, using human-machine interface (HMI) only.

This late consideration of human factors can greatly reduce the potential for achieving the highest levels of safety and reliability, even though effective solutions may be proposed at the HMI level. However, feedback from operational experience, such as in safety significant events reports, shows that most of the situations that seriously challenge a plant operators' performance and further plant safety and/or productivity originate in more fundamental reactor or reactor system design deficiencies, not just in I&C or HMI deficiencies. For cost and performance-effective design, human factors requirements must be specified early and implemented at the beginning of the design process.

Human Factors Objectives in the Design

Multilayers and Global Sequential Design Process

The design of a nuclear power plant can be considered a sequential process, during which successive "layers" are added to the initial choice of the fundamental reactor technology (and for other facilities, the fundamental process technology). Figure G-1 illustrates this sequential process.

1. The first design consideration is choosing the basic reactor technology for the central kernel of the plant, such as water- or gas-cooled. This choice needs to match, as closely as possible, the global techno-economical objectives assigned to the project, such as refueling and waste processing costs limitations, initial investment minimization, etc.

2. The second design consideration is the various systems connected to the central kernel, which ensure the global control of the plant under various conditions (normal or abnormal). The degree of freedom still available to the designers at the plant systems level can be exploited to optimize the safety and productivity objectives of the plant.

3. The third design consideration is the I&C, which provides an effective control of the various plant actuators that give access to the plant information. Plant automation decisions are generally made at this level.

4. The last design consideration is the plant HMI, which enables the operators to monitor the evolution of the plant and take active control of it within the limits of actions allowed by the automatic control systems.

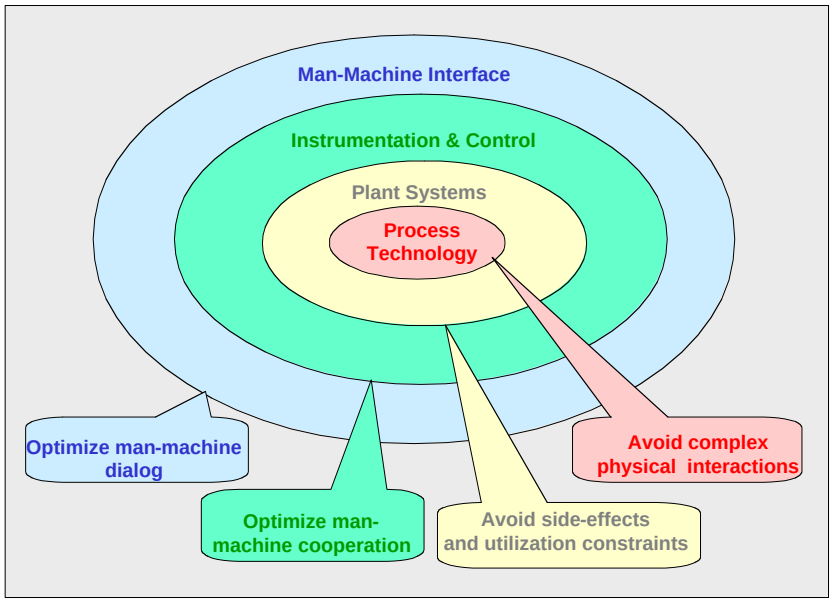

Figure G-1. The multilayer process and associated human factors objectives in nuclear power plant design.

This design process is highly iterative between the various phases, having been viewed as a "design spiral" by some. Certainly, revisions can and do occur when difficulties are experienced during development of one of the layers. For example, in the pressurized reactor concept, limitations (technical or economical) on the design of the volumetric control system might lead designers to reconsider the pressurizer volume to shift the performance requirements placed on this system. But as the design advances, it becomes more and more difficult and expensive to change the initial design decisions, since such design modifications then affect a larger and more detailed set of subsequent design decisions that may also require review and modification. Therefore, it is unrealistic to expect designers to significantly alter the design for human factors issues, should such be detected in later phases (I&C or HMI) of the design process. It is far much more desirable to have a systematic and effective approach to anticipate and correct human factors issues in the early stages of the design process.

Human Factors Objectives In Design

Typically, I&C and HMI designers have implicitly accepted complex plant management constraints resulting from the basic design choices, and tried to solve them by the generalized recourse to automation during the I&C level of the plant design process, or to advanced operational aids during the HMI level to compensate for human performance limitations. However, both of these solutions decouple the operators from the real decisional roles, and thus, place the total operational responsibility on designers, who, on another hand, are probably not able to anticipate all the situations that could occur under the complex actual conditions of plant operations.

A better solution would be avoiding design choices that create system responses that exceed the capabilities of human performance and lead to cognitively challenging situations for the operators. This can be done by the a priori expression of human factor objectives allocated to each phase of the design, including the earliest phases as depicted in Figure G-1:

- At the basic concept design level, the human factors operational objective should be to avoid complex physical interactions or dynamic behaviour within the main processes of the plant (like for

example, complex and unstable reactivity effects in the RBMK cores, at low power rates). The human factors maintenance objective should be to ensure physical configuration for ease and effectiveness of required maintenance. Here it is quite important to note that the Generation IV Final Screening process for SR focused on this objective, by giving higher scores to reactor concepts that achieved the major safety functions of reactivity control, decay heat removal, and radionuclide confinement by simple and intrinsic mechanisms. This provides a strong foundation for achieving human factors objectives for Generation IV nuclear energy systems, if the subsequent design process also considers human factors objectives appropriately.

- At the plant (safety) systems design level, the human factors objective should be to limit side effects and utilisation constraints that lead to more complexity in the operational strategy, and to avoid carry-forward design constraints on the plant operation (for example via the maintenance and testing priorities).

- At the I&C design level, the human factors objective should be the optimization of cooperation between operators and automatic control systems; for example, by using an effective human-centred automation approach and a systemic view of the global plant operating system (this is global optimization of the "hybrid system" formed by the operating crews, I&C and HMI, and the operating rules).

- And finally, at the HMI design level, the human factors objective should remain the optimization of human-machine dialogs. In general this last optimization is the only human factors objective that has been systematically considered in the design of the present generation plants.

Crosscut R&D Needs in the Human Factors Domain

In conclusion, instead of allocating to the human factors specialists the difficult, and not always effective, mission of compensating for the plant design deficiencies at the I&C and HMI design levels, better results will be achieved from adopting a concurrent engineering organization, in which human factors specialists and experienced operators become actively involved in design choices early in the design process. This recommendation overlaps the generic recommendation of the RSCG, that systematic reviews of all Generation IV concepts be performed by experts in each of the seven SR topical areas. The counterpart of this active involvement of the human factors specialists in Generation IV concept design is that they must be able to express synthetic human factors requirements and criteria that are in balance with the techno-economical factors that designer's must also consider. In other words, HMI specialists must take an active part in the decision process, but their recommendations must be based on quantitative criteria that can enable decisions between alternative design solutions on a cost-benefits basis.

As far as Generation IV is concerned, this HMI expert review and input could be particularly helpful during the viability analysis of the specific concepts.

Synthetic and Quantitative Design-Based Human Factors Criteria

One of the main objectives of crosscut R&D in the human factors domain should be to identify and characterize the plant and systems design features that influence human performance in operation, and then, to create quantitative human factors criteria that will enable effective comparison of Generation IV concepts and original design decisions.

In the human factors community, specialists are generally reluctant to adopt quantitative approaches to characterize human activity. Their reservations find justification in the fact that the human performance depends on many context-influencing factors that are difficult to identify or to represent with

generic models. That is why the human performance assessment methodologies based on generic models such as SWAIN curves that link performance to time delays and complexity, tend to be replaced progressively by more sophisticated and more specific methods, taking the real cognitive situations and the influence of the context into account. In the case of existing plants risk assessment, this tendency to search for a more realistic assessment of the human contribution, based on the utilization of the experience feedback, is particularly pertinent as far as the objective to have as precise an assessment as possible. But this best estimate approach is not easily usable as a support for design activities for the following reasons:

1. First, because human resource analysis involves complex models and extensive development, which are generally incompatible with the major priorities (cost, delays, etc.) of a design project

2. Second, because they require precise design data that are not always available in the early phases of the design

3. Third, because, in the case of new innovative projects, the experience feedback from previous plants is not always relevant

4. Finally, because, in the case of design studies, what is needed most is a simple method to enable comparisons between alternative solutions, rather than a best-estimate method aiming at an absolute rating of the residual risk.

For these reasons, it would be preferable to adopt a simpler and more generic approach to determine the impact of design features on human reliability, based on the dominant factors of influence, that can be linked to performance shaping factors used in some human reliability analysis methods such as the "technique for human error rate prediction." Globally, these factors can be related to system complexity (structural, functional and dynamic) and system times constraints that are directly influenced by design options, particularly those selected in the earliest stages of design development. Some of the second generation HRA methods,[1,2,3] with their focus on context, have developed catalogs of special conditions that make human cognitive error more likely. These could form a starting point for the needed development of a human factors design tool.

Characterization and Optimization of the Positive Role of Humans in Operation

The decision to maintain humans in an active role in the management of future plants and decisions that set their actual level of responsibility should be based on objective evidence for positive contributions to plant SR. We have seen, on a global basis, that design decisions can significantly impact human performance in operation. This human performance can be considered from two points of view:

- The classical point of view considers the negative aspect of human performance through the contribution of human factors to the overall risk. It is the domain traditionally covered by probabilistic risk assessment studies and their human factors branch, the human reliability

---

1. Hollnagel, E. Cognitive Reliability and Error Analysis Method: CREAM, Elsevier Science Inc., New York, 1998.

2 ."Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)," NUREG-1624, Rev. 1, U.S. Nuclear Regulatory Commission, May 2000.

3. MERMOS

assessment. Probabilistic risk assessments that crosscut R&D topics focus particularly in this domain.

- The less formalized point of view aims at characterizing the positive impact of human actions, particularly on reliability, but also on safety.

The fundamental point is that searching for human factor optimization in plant designs cannot be restricted to the minimization of human factor contribution to the risk, because this would sooner or later lead to separating humans from the responsibility of plant operations. Rather, in the optimization process, one must try to keep an optimal balance between both positive and negative contributions of human factors.

In addition to the evaluation of the negative impact of human factors on risk, which has been encouraged by licensing priorities, the positive impact of humans on safety and operation efficiency is not so well characterized; although, a consensus has emerged within the human factors community to acknowledge this positive effect.

The main argument is that the humans are a critical defense-line against unanticipated situations, that are situations against which designers did not provide any (rule-based) management strategy. In such situations, challenging either safety or availability, it is expected that the humans will be able to engage some forms of knowledge-based cognitive strategies, in order to solve the problems. And this admission of the limits of the designer's ability to anticipate all the situations is probably the main argument to maintain a role for humans in plant operation, at a time when technology would permit the design of totally autonomous plants.

The problem is to find some evidence of this positive role of humans, particularly on plant safety, and to identify those design features that facilitate this knowledge-based management. The approach of this problem is more difficult than in the case of the negative impacts, because the experience feedback on these favorable operator's behaviors is generally not directly available: generally, experience feedback processes are more oriented towards the identification and correction of wrong practices than towards the promotion of good practices. That is why it is so difficult to obtain information about these situations, during which human action and decision have a positive impact on the safety or availability of the plants. Thus, without this objective information source, it appears to be quite impossible to characterize the mechanisms (positive performance shaping factors) favoring efficient knowledge-based strategies in case of unanticipated situations.

This is why an important human factors R&D objective in this domain is to organize the collection and analysis of this positive experience feedback at a wide scale.

Otherwise, we will be reduced to base our reflection on expert statements or common sense considerations like the one that makes us think that, in the domain of design-based factors (which are not the only ones to be considered, whereas organizational and cultural factors are expected to play a prominent role), process complexity, or rather simplicity, will also play a important role in the reinforcing of human performance at the high cognitive levels.

Human Factors at the I&C and HMI Design Level

Provided the fact that an effective minimization of process design-induced constraints has been obtained, thanks to the human-based design approach presented previously, the further human factors optimization in the design of I&C and HMI doesn't require particular research effort, as some effective

human-centred design methodologies are already available for the design of the I&C, the control rooms and the operating supports (HMI, procedures, etc.).

These methodological advances are, for example:

- *Human-centred automation approaches*, aiming at basing automation decisions on the optimization of operators' plant awareness, instead of technical feasibility considerations.

- *Systemic approaches* for the optimum design of the global hybrid operating system formed by the operating crews (organization and training), the technical means (automatic controls, operators aids, etc.), and the operational documentation (procedures). The basic principle is to try to adopt a global optimization approach instead of trying to optimize separately the various components.

- *Functional approaches* for plant operations organization (procedures and HMI structuring, crew organization, etc.), putting emphasis on the plant safety and availability functional objectives instead of the essentially topologic and organic view prevailing in the present operating practices.

All these I&C and HMI design approaches based on the optimization of human performance in operation are now rather well formalized, if not standardized. IEC 964 and ISO 11064 standards are some examples of human factors design guidelines promoting such human-centred design approaches. These standards should be applied to support the design of Generation IV nuclear energy systems.